What is claimed is:

1. A method for preventing an illegal use of a mobile communication terminal comprising the steps of:

transmitting a short message service (SMS) message to a lost terminal when a user requests a phone-locking service; and

analyzing the received SMS message to set a phone-locking state for the lost terminal.

2. The method of claim 1, wherein the SMS message includes a header and a ciphered string.

3. The method of claim 1, wherein the phone-locking function setting step comprises:

checking whether a ciphered string is contained in the SMS message;

discriminating a type of the ciphered string; and

setting the lost terminal to a phone-locking state, if the ciphered string is for a phone-locking use.

4. The method of claim 3, wherein the phone-locking state setting step comprises:

reading a lock code from a memory;

enabling a variable value for the phone-locking; and

setting the phone-locking state on the basis of the read lock code and displaying a phone-locking state on an LCD screen.

5. A method for preventing an illegal use of a mobile communication terminal comprising the steps of:

transmitting an SMS message to a lost terminal from an exchange when a phone-locking service is requested; and

analyzing the received SMS message and turning off an LCD power by the lost terminal.

6. The method of claim 5, wherein the SMS message includes a header and a ciphered string.

7. The method of claim 5, wherein the LCD power turning off step comprises:

checking whether a ciphered string exists in the SMS message;

discriminating a type of the ciphered string contained in the SMS message; and

turning off the LCD power, if the type of the ciphered string is for an LCD power OFF use.

8. A method for preventing an illegal use of a mobile communication terminal comprising:

a first step in which when a user requests a phone-locking service, an SMS message is transmitted to the lost terminal; and

a second step in which the received SMS message is analyzed to set a phone-locking function or turn off an LCD power.

9. The method of claim 8, wherein the SMS message includes a header and a ciphered string.

10. The method of claim 8, where the second step comprises:

checking whether a ciphered string is contained in the SMS message;

discriminating a type of the ciphered string contained in the SMS message; and

setting a phone-locking or turning off the LCD power according to the discriminated ciphered string type.

11. The method of claim 10, wherein the phone-locking state setting step comprises:

reading a lock code if the ciphered string is for a phone-locking use;

enabling a variable value for a phone-locking; and

setting a phone-locking state on the basis of the read lock code and displaying a phone-locking state on the LCD screen.

12. The method of claim 10, wherein the LCD power turning off step comprises:

controlling a general purpose input/output (GPIO) port of a mobile station modem (MSM) and cutting off power applied to the LCD; and

converting a data variable of a memory.

13. The method of claim 10, wherein, if no ciphered string is contained in the SMS message, a general SMS message processing is performed.

14. A method for preventing an illegal use of a mobile communication terminal comprising the steps of:

receiving an SMS message from a base station;

checking whether a ciphered string exists in the received SMS message;

discriminating a type of the ciphered string if a ciphered string exists in the SMS message; and

setting a phone-locking or turning off an LCD power for the lost terminal according to the discriminated ciphered string type.

15. The method of claim 14, wherein the SMS message includes a header and a ciphered string.

16. The method of claim 14, wherein the phone-locking state setting step comprises:

reading a lock code from the memory if the ciphered string is for a phone-locking use;

enabling a variable value for the phone-locking; and

setting the phone-locking state on the basis of the read lock code and displaying the phone-locking state on the LCD screen.

17. The method of claim 14, wherein the LCD power turning off step comprises:

controlling the GPIO port of the MSM and cutting off power applied to the LCD; and

converting a data variable of the memory as the power is cut off.

18. The method of claim 14, wherein, if no ciphered string is contained in the SMS message, a general SMS message processing is performed.